FOR PUBLICATION

UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.
NICHOLAS MIDDLETON,

Defendant-Appellant.

No. 99-10518

D.C. No.
CR-98-00167-WHO

OPINION

Appeal from the United States District Court
for the Northern District of California
William H. Orrick, Jr., District Judge, Presiding

Argued and Submitted
September 12, 2000--San Francisco, California

Filed November 16, 2000

Before: Susan P. Graber, Raymond C. Fisher, and
Marsha S. Berzon, Circuit Judges.

Opinion by Judge Graber

COUNSEL

David J. Cohen, Cohen & Paik, San Francisco, California, for the defendant-appellant.

J. Douglas Wilson, Assistant United States Attorney, Chief, Appellate Section, San Francisco, California, for the plaintiff-appellee.

OPINION

GRABER, Circuit Judge:

Defendant Nicholas Middleton challenges his conviction for intentionally causing damage to a "protected computer" without authorization, in violation of 18 U.S.C. § 1030(a)(5)(A). Defendant asks us to interpret the statute, which prohibits conduct causing damage to "one or more individuals," 18 U.S.C. § 1030(e)(8)(A), to exclude damage to a corporation. Defendant also argues that the trial court incorrectly instructed the jury on the "damage " element of the offense and that the government presented insufficient evidence of the requisite amount of damage. We disagree with each of Defendant's contentions and, therefore, affirm the conviction.

FACTUAL AND PROCEDURAL BACKGROUND[1]

Defendant worked as the personal computer administrator for Slip.net, an Internet service provider. His responsibilities included installing software and hardware on the company's computers and providing technical support to its employees. He had extensive knowledge of Slip.net's internal systems, including employee and computer program passwords. Dissatisfied with his job, Defendant quit. He then began to write threatening e-mails to his former employer.

Slip.net had allowed Defendant to retain an e-mail account as a paying customer after he left the company's employ. Defendant used this account to commit his first unauthorized act. After logging in to Slip.net's system, Defendant used a computer program called "Switch User" to switch his account to that of a Slip.net receptionist, Valerie Wilson. This subterfuge allowed Defendant to take advantage of the benefits and privileges associated with that employee's account, such as creating and deleting accounts and adding features to existing accounts.

Ted Glenwright, Slip.net's president, discovered this unauthorized action while looking through a "Switch User log," which records all attempts to use the Switch User program.

Glenwright cross-checked the information with the company's "Radius Log," which records an outside user's attempt to dial in to the company's modem banks. The information established that Defendant had connected to Slip.net.'s computers and had then switched to Wilson's account. Glenwright immediately terminated Defendant's e-mail account.

[1] Because a jury convicted Defendant, we view the evidence in the light most favorable to the government. United States v. Cuevas, 847 F.2d 1417, 1421 (9th Cir. 1988).

Nevertheless, Defendant was able to continue his activities. Three days later, he obtained access to Slip.net's computers by logging in to a computer that contained a test account and then using that test account to gain access to the company's main computers. Once in Slip.net's main system, Defendant accessed the account of a sales representative and created two new accounts, which he called "TERPID" and"SANTOS." Defendant used TERPID and SANTOS to obtain access to a different computer that the company had named "Lemming." Slip.net used Lemming to perform internal administrative functions and to host customers' websites. Lemming also contained the software for a new billing system. After gaining access to the Lemming computer, Defendant changed all the administrative passwords, altered the computer's registry, deleted the entire billing system (including programs that ran the billing software), and deleted two internal databases.

Glenwright discovered the damage the next morning. He immediately contacted the company's system administrator, Bruno Connelly. Glenwright and Connelly spent an entire weekend repairing the damage that Defendant had caused to Slip.net's computers, including restoring access to the computer system, assigning new passwords, reloading the billing software, and recreating the deleted databases. They also spent many hours investigating the source and the extent of the damage. Glenwright estimated that he spent 93 hours repairing the damage; Connelly estimated that he spent 28 hours; and other employees estimated that they spent a total of 33 hours. Additionally, Slip.net bought new software to replace software that Defendant had deleted, and the company hired an outside consultant for technical support.

Defendant was arrested and charged with a violation of 18 U.S.C. § 1030(a)(5)(A). He moved to dismiss the indictment, arguing that Slip.net was not an "individual" within the meaning of the statute. The district court denied the motion, holding that "the statute encompasses damage sustained by a

business entity as well as by a natural person." United States v. Middleton, 35 F. Supp. 2d 1189, 1192 (N.D. Cal. 1999).

The case was then tried to a jury. Defendant filed motions for acquittal, arguing that the government had failed to prove that Slip.net suffered at least $5,000 in damage. The district court denied the motions. Defendant requested a jury instruction on the meaning of "damage." This request, too, was denied, and the court gave a different instruction.

The jury convicted Defendant. The district court sentenced him to three years' probation, subject to the condition that he serve 180 days in community confinement. The court also ordered Defendant to pay $9,147 in restitution. This timely appeal ensued.

STANDARDS OF REVIEW

We review de novo the district court's interpretation of a statute. United States v. Frega, 179 F.3d 793, 802 n.6 (9th Cir. 1999). We also review de novo whether a jury instruction misstates the elements of a statutory crime. Id. at 806 n.16. We review a challenge to the sufficiency of the evidence by examining the evidence in the light most favorable to the prosecution and determining whether any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt. Jackson v. Virginia, 443 U.S. 307, 319 (1979).

DISCUSSION

A. "One or More Individuals"

Title 18 U.S.C. § 1030(a)(5)(A) prohibits a person from knowingly transmitting "a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer." A "protected computer" is a computer "which is used in inter-

state or foreign commerce or communication." 18 U.S.C.

§ 1030(e)(2)(B). Defendant concedes that Slip.net's computers fit within that definition. The statute defines"damage" to mean "any impairment to the integrity or availability of data, a program, a system, or information, that causes loss aggregating at least $5,000 in value during any 1-year period to one or more individuals." 18 U.S.C. § 1030(e)(8)(A). Defendant argues that Congress intended the phrase "one or more individuals" to exclude corporations. We disagree.

"In interpreting a statute, we look first to the plain language of the statute, construing the provisions of the entire law, including its object and policy, to ascertain the intent of Congress." United States v. Mohrbacher, 182 F.3d 1041, 1048 (9th Cir. 1999) (citation and internal quotation marks omitted). When a statutory term is undefined, we endeavor to give that term its ordinary meaning. Id. We are instructed to avoid, if possible, an interpretation that would produce"an absurd and unjust result which Congress could not have intended." Clinton v. City of New York, 524 U.S. 417, 429 (1998).

According to Defendant, in common usage the term"individuals" excludes corporations. He notes that the"Dictionary Act," 1 U.S.C. § 1, which provides general rules of statutory construction, defines the word "person" to include "corporations, companies, associations, firms, partnerships, societies, and joint stock companies, as well as individuals. " That definition, argues Defendant, implies that the word"person" includes "corporations," but that the word"individuals" does not. Defendant reasons that, if Congress had intended § 1030(a)(5)(A) to cover damage to corporations, Congress would have used the word "persons," not "individuals." For several reasons, we are not persuaded.

We examine first the ordinary meaning of "individuals." That word does not necessarily exclude corporations. Webster's Third New Int'l Dictionary 1152 (unabridged ed. 1993) provides five definitions of the noun "individual," the

first being "a single or particular being or thing or group of beings or things." (Emphasis added.) To the extent that a word's dictionary meaning equates to its "plain meaning," a corporation can be referred to as an "individual. " Cf. United States v. Miguel, 111 F.3d 666, 670 (9th Cir. 1997) (using a dictionary to define "contemporaneous").

Neither is "individual" a legal term of art that applies only to natural persons. As Black's Law Dictionary 773 (6th ed. 1990) states:

> **Individual.** As a noun, this term denotes a single person as distinguished from a group or class, and also, very commonly, a private or natural person as distinguished from a partnership, corporation, or association; but it is said that this restrictive signification is not necessarily inherent in the word, and that it may, in proper cases, include artificial persons.

(Emphasis added.) See also Black's Law Dictionary 777 (7th ed. 1999) (stating that "individual" refers to"an indivisible entity" or a "single person or thing"). Because "individual" as a general legal term does not exclude corporations, we next consider applicable precedent.

In Clinton, the Supreme Court held that Congress intended to include corporations within a provision of the Line Item Veto Act that authorized "any individual adversely affected" to challenge the Act's constitutionality. 524 U.S. at 428 (emphasis added). The Court examined the purpose of the provision (to allow expedited judicial review of the Line Item Veto Act) and determined that Congress could not have intended that only natural persons be able to demand expedited review. Id. at 429. That interpretation, noted the Court, would produce an "absurd and unjust result which Congress could not have intended." Id.

So, too, here. Defendant was convicted of violating § 1030(a)(5)(A), which criminalizes damage to"protected computers." A "protected computer" is a computer that is "used in interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B). A large number of the computers that are used in interstate or foreign commerce or communication are owned by corporations. Cf. S. Rep. No. 104-357, pt. II (1996) (noting that "computers continue to proliferate in businesses and homes"). It is highly unlikely, in view of Congress' purpose to stop damage to computers used in interstate and foreign commerce and communication, that Congress intended to criminalize damage to such computers only if the damage is to a natural person. Defendant's interpretation would thwart Congress' intent.

Defendant's interpretation also ignores the context in which the term "individual" appears. It is true that the Dictionary Act's definition of "person" implies that the words "corporations" and "individuals" refer to different things. But the Dictionary Act instructs us not to use its definitions if "the context indicates otherwise." 1 U.S.C. § 1. Context refers to "the text of the Act of Congress surrounding the word at issue, or the texts of other related congressional Acts." *Rowland v. California Men's Colony*, 506 U.S. 194, 199 (1993); *see id.* at 198-200 (interpreting the word "person," as used in 28 U.S.C. § 1915, to mean natural persons only). An examination of 18 U.S.C. § 1030 in its entirety uncovers further evidence that Congress did not, as Defendant argues, intend to use the word "individuals" to mean natural persons only, and the word "person" to mean natural persons *and* corporations.

As noted, 18 U.S.C. § 1030(e)(8)(A) defines "damage" to mean "any impairment to the integrity or availability of data, a program, a system, or information that causes loss aggregating at least $5,000 . . . to one or more individuals." Section 1030(e)(8)(C) provides an alternative definition of damage: any impairment to a system "that causes physical injury to any person." Under Defendant's theory, corporations could suffer "damage" as defined in § 1030(e)(8)(C), because a corporation is a "person." Corporations, however, cannot suffer "physical injury." *See Black's Law Dictionary* 1147 (defining "physical injury" as "[b]odily harm or hurt"). If Congress had meant to incorporate the Dictionary Act's definition of "person" (and, by extension, Defendant's definition of "individual"), § 1030(e)(8)(C) should read, "that causes physical injury to any individual." But it does not. In context, it appears that Congress used "individuals" and "person" in a non-technical manner, without reference to the Dictionary Act.

Defendant also relies on the statute's legislative history. We have examined that history, but conclude that the statute's history confirms our reading of the word "individuals." Congress originally enacted the Computer Fraud and Abuse Act in 1984. Pub. L. No. 98-473, tit. II, § 2102(a), Oct. 12, 1984. The 1990 version of § 1030(a)(5)(A) prohibited conduct that damages a "Federal interest computer" and"causes loss to one or more others of a value aggregating $1,000 or more." A "Federal interest computer" was defined as a computer owned or used by the United States Government or a financial institution, or "one of two or more computers used in committing the offense, not all of which are located in the same State." 18 U.S.C. § 1030(e)(2)(A) & (B) (1990). In 1994, Congress replaced the term "Federal interest computer" with the phrase "computer used in interstate commerce or communication" and changed the damage provision to read, "causes loss or damage to one or more other persons of value aggregating $1,000 or more." 18 U.S.C. § 1030(a)(5)(A)(ii)(II)(aa) (1995). Before the 1994 amendment, a hacker could escape the statute's prohibitions by containing activities within a single state. Congress' 1994 amendment attempted to"broaden the statute's reach." S. Rep. No. 104-357, pt. IV(E) (discussing 1994 amendment). Congress' 1994 amendments also added a private cause of action for victims of computer crime. 18 U.S.C. § 1030(g).

In 1996, Congress amended § 1030(a)(5) to its current form, using the term "protected computer" and concomitantly expanding the number of computers that the statute"protected." 18 U.S.C. § 1030(a)(5) & (e)(2).[2] The 1996 amendments also altered the definition of damage to read, "loss aggregating at least $5,000 in value during any 1-year period to one or more individuals." 18 U.S.C. § 1030(e)(8)(A). We have found no explanation for this change. We do not believe, however, that this change evidences an intent to limit the statute's reach.

To the contrary, Congress has consciously broadened the statute consistently since its original enactment. The Senate Report on the 1996 amendments notes:

> As intended when the law was originally enacted, the Computer Fraud and Abuse statute facilitates addressing in a single statute the problem of computer crime . . . . As computers continue to proliferate in businesses and homes, and new forms of computer crimes emerge, Congress must remain vigilant to ensure that the Computer Fraud and Abuse statute is up-to-date and provides law enforcement with the necessary legal framework to fight computer crime.

[2] The 1996 amendments corrected deficiencies in the 1990 version of the statute and the 1994 version. In 1994, when Congress substituted the

phrase "computer used in interstate commerce or communication" for "Federal interest computer," it inadvertently removed protection from those computers belonging to or used by the United States Government or a financial institution, but not used in interstate commerce. *See* S. Rep. No. 104-357. The 1996 amendments included within the definition of "protected computer" those computers used in interstate commerce or communication, as well as computers "exclusively for the use of a financial institution or the United States Government, or. . . used by or for a financial institution or the United States Government and the conduct constituting the offense affects the use." 18 U.S.C.§ 1030(e)(2)(A).

S. Rep. No. 104-357, pt. II (emphasis added). The report instructs that "the definition of `damage' is amended to be sufficiently broad to encompass the types of harm against which people should be protected." *Id.* pt. IV(1)(E). The report notes that the interaction between § 1030(a)(5)(A) (the provision that prohibits conduct causing damage) and § 1030(e)(8) (the provision that defines damage) will prohibit a hacker from stealing passwords from an existing log-on program, when this conduct requires "all system users to change their passwords, *and requires the system administrator to devote resources to resecuring the system*. . . . If the loss to the victim meets the required monetary threshold, the conduct should be criminal, and the victim should be entitled to relief." *Id.* (emphasis added). The reference to a "system administrator" suggests that a corporate victim is involved. That is, if Congress intended to limit the definition of the crime to conduct causing financial damage to a natural person only, its report would not use the example of a"system administrator" devoting resources to fix a computer problem as illustrative of the "damage" to be prevented and criminalized. The Senate Report's reference to the proliferation of computers in businesses as well as homes provides additional evidence of the Senate's intent to extend the statute's protections to corporate entities.

On the basis of the statutory text taken in context, the Supreme Court's *Clinton* decision, and the statute's purpose and legislative history, we conclude that 18 U.S.C. § 1030(a)(5) criminalizes computer crime that damages natural persons and corporations alike. The district court did not err in so ruling.

B. *Jury Instructions on "Damage"*

Defendant next argues that the district court instructed the jury improperly on the definition of "damage. " Defendant requested this instruction: "Damage does not include expenses relating to creating a better or making a more secure system than the one in existence prior to the impairment." The court refused the request and gave a different instruction. The court explained to the jury that "damage" is an impairment to Slip.net's computer system that caused a loss of at least $5,000. The court continued:

> The term "loss" means any monetary loss that Slip.net sustained as a result of any damage to Slip.net's computer data, program, system or information that you find occurred.
>
> And in considering whether the damage caused a loss less than or greater than $5,000, you may consider any loss that you find was a natural and foreseeable result of any damage that you find occurred.
>
> In determining the amount of losses, you may consider what measures were reasonably necessary to restore the data, program, system, or information that you find was damaged or what measures were reasonably necessary to resecure the data, program, system, or information from further damage.

"In reviewing jury instructions, the relevant inquiry is whether the instructions as a whole are misleading or inadequate to guide the jury's deliberation." United States v. Dixon, 201 F.3d 1223, 1230 (9th Cir. 2000). In this case, the district court's instructions on "damage" and "loss " correctly stated the applicable law. Defendant concedes that "damage" includes any loss that was a foreseeable consequence of his criminal conduct, including those costs necessary to"resecure" Slip.net's computers. He does not argue, therefore, that the court misstated the law.

Defendant contends instead that the court's instruction might have led the jury to believe that it could consider the cost of creating a better or more secure system and that his proposed additional instruction was needed to avoid that possibility. The district court's instruction, when read in its entirety, adequately presented Defendant's theory. The court instructed the jury that it could consider only those costs that were a "natural and foreseeable result" of Defendant's conduct, only those costs that were "reasonably necessary," and only those costs that would "resecure" the computer to avoid "further damage." That instruction logically excludes any costs that the jury believed were excessive, as well as any costs that would merely create an improved computer system unrelated to preventing further damage resulting from Defendant's conduct. In particular, the term "resecure " implies making the system as secure as it was before, not making it more secure than it was before. We presume that the jury followed the court's instructions. United States v. Montgomery, 150 F.3d 983, 997 (9th Cir. 1998).

Because "the district court's instructions fairly and adequately covered the elements of the offense, we review the instruction's `precise formulation' for an abuse of discretion." United States v. Knapp, 120 F.3d 928, 930 (9th Cir. 1997). The district court in this case did not abuse its discretion in rejecting Defendant's "precise formulation" of the definition of "damage." See United States v. Smith , 217 F.3d 746, 750 (9th Cir. 2000) (stating that "it is not required that a jury be instructed in line with the chosen words of the accused").

C. Sufficiency of the Evidence

Defendant's final argument is that the government presented insufficient evidence of the requisite $5,000 in damage. The government computed the amount of damage that occurred by multiplying the number of hours that each employee spent in fixing the computer problems by their respective hourly rates (calculated using their annual salaries), then adding the cost of the consultant and the new software. The government estimated the total amount of damage to be $10,092. Defendant and the government agree that the cost of Glenwright's time made up the bulk of that total.

Defendant observes that Slip.net paid Glenwright a fixed salary and that Slip.net did not pay Glenwright anything extra to fix the problems caused by Defendant's conduct. There also is no evidence, says Defendant, that Glenwright was diverted from his other responsibilities or that such a diversion caused Slip.net a financial loss. Defendant argues that, unless Slip.net paid its salaried employees an extra $5,000 for the time spent fixing the computer system, or unless the company was prevented from making $5,000 that it otherwise would have made because of the employees' diversion, Slip.net has not suffered "damage" as defined in the statute. We disagree.

In *United States v. Sablan*, 92 F.3d 865, 869 (9th Cir. 1996), this court held that, under the Sentencing Guidelines for computer fraud, it was permissible for the district court to compute "loss" based on the hourly wage of the victim bank's employees. The court reasoned, in part, that the bank would have had to pay a similar amount had it hired an outside contractor to repair the damage. *Id.* at 870. Analogous reasoning applies here. There is no basis to believe that Congress intended the element of "damage" to depend on a victim's choice whether to use hourly employees, outside contractors, or salaried employees to repair the same level of harm to a protected computer. Rather, whether the amount of time spent by the employees and their imputed hourly rates were reasonable for the repair tasks that they performed are questions to be answered by the trier of fact.

Our review of the record identifies sufficient evidence from which a rational trier of fact could have found that Slip.net suffered $5,000 or more in damage. Glenwright testified that he spent approximately 93 hours investigating and repairing the damage caused by Defendant. That total included 24 hours investigating the break-in, determining how to fix it, and taking temporary measures to prevent future break-ins. Glenwright testified that he spent 21 hours recreating deleted databases and 16 hours reloading and configuring the billing software and its related applications. Glenwright estimated that his time was worth $90 per hour, based on his salary of $180,000 per year. He also testified, among other things, that he did not hire an outside contractor to repair the damage because he believed that he, as a computer expert with a pre-existing knowledge of the customized features of his company's computers, could fix the problems more efficiently. It is worth noting that, because the jury had to find only $5,000 worth of damage, it could have discounted Glenwright's number of hours or his hourly rate considerably and still have found the requisite amount of damage.

Other Slip.net employees testified to the hours that they spent fixing the damage caused by Defendant, and to their respective salaries. The government then presented expert testimony from which a jury could determine that the time spent by the employees was reasonable. Defendant cross-examined the government's witnesses on these issues vigorously, and he presented contrary expert testimony. By the verdict, the jury found the government witnesses' testimony to be more credible, a finding that was within its power to make. We hold, on this record, that the conviction was not based on insufficient evidence.

AFFIRMED.